University of Westminster
School of Computer Science and Engineering

6COSC002W Security and Forensics Assignment (2019/20)

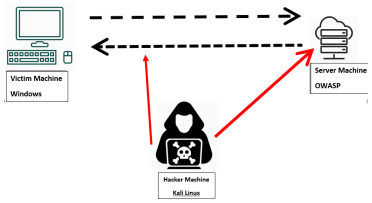
Module leader	Ayman El Hajjar
Unit	Coursework
Weighting:	50%
Qualifying mark	30%
Description	Scenario based lab report
Learning Outcomes Covered in this Assignment:	LO1: synthesise emerging trends through engagement and analysis with current research; LO4: carry out basic forensic analysis of a computer system and the afterfacts involved; LO5: synthesise emerging trends through engagement and analysis with current research
Handed Out:	04 February 2020
Due Date	Tuesday 07 April 2020 at 1:00 PM
Expected deliverables	Single Report
Method of Submission:	Electronic submission on tunrnitin (in PDF format) name your file with your student number and the module code. i.e.: W000000000 6COSC002W
Type of Feedback and Due Date:	Written feedback and marks will be given 15 working day (3 Weeks) after the submission deadline. **All marks will remain provisional until formally agreed by an Assessment Board.**

Assessment regulations

Refer to section 4 of the "How you study" guide for undergraduate students for a clarification of how you are assessed, penalties and late submissions, what constitutes plagiarism etc.

Penalty for Late Submission
If you submit your coursework late but within 24 hours or one working day of the specified deadline, 10 marks will be deducted from the final mark, as a penalty for late submission, except for work which obtains a mark in the range 40 – 49%, in which case the mark will be capped at the pass mark (40%). If you submit your coursework more than 24 hours or more than one working day after the specified deadline you will be given a mark of zero for the work in question unless a claim of Mitigating Circumstances has been submitted and accepted as valid.
It is recognised that on occasion, illness or a personal crisis can mean that you fail to submit a piece of work on time. In such cases you must inform the Campus Office in writing on a mitigating circumstances form, giving the reason for your late or non-submission. You must provide relevant documentary evidence with the form. This information will be reported to the relevant Assessment Board that will decide whether the mark of zero shall stand. For more detailed information regarding University Assessment Regulations, please refer to the following website:**http://www.westminster.ac.uk/study/current-students/resources/academic-regulations**

Coursework description



You are expected to use the lab results you have obtained during your lab classes in order to be able to write a penetration testing report for your scenario.

To be able to complete your assessment for your allocated scenario, you will need to complete your penetration testing on the company. You will need to complete the labs in order to be able to answer the questions for each task. You will have three VMs, the Victim machine (**Windows**), the server machine (**OWASP**) and the hacker machine (**Kali Linux**).

Scenarios

IMPORTANT GUIDELINES

- **Each of you is allocated a scenario. The allocation of the scenarios is on blackboard. (You can click here to open it)**
- **Failing to follow this guideline will result in you getting a penalty of 20% of your mark.**
- **You will need to refer to the scenarios document to find the scenario allocated for you.**

Requirements and Deliverables

Now you have completed your assessment of the scenario application and identified their vulnerabilities and weaknesses. You are now expected to document your findings in a report. Your report should contain all the information below that are required by the company that hired you. .

Report requirements for your client

A- Information gathering – Social engineering and nmap

(1) Identify the ports you found in the lab running on the server machine and briefly explain what threats those open ports bring to your scenario. [8 marks]

(2) identify two services running on the server machine that should be priority to protect. Document your security concerns if you have any and justify your answers [6 marks]

(3) Once you identify the services on your machine, research three internet vulnerabilities related to those services. (look for versions, number of users, etc..)[6 marks]

(4) Pick the four least secure services running on the server machine and explain the danger posed by each of them. Document your security concerns if you have any. [6 marks]

B- Finding and exploiting vulnerabilities

(1) Identify if the application is vulnerable to data tampering and exploit it if possible. [5 marks]

(2) Identify if the application is vulnerable to SQL injection and exploit it if possible [5 marks]

(3) Identify if the application is vulnerable to XSS vulnerability and exploit it if possible. [5 marks]

(4) Can you identify any other vulnerability? [5 marks]

C- Man in the middle attacks and social engineering

(1) If a client is connected to the server while you are testing the environment, identify what are the information that can be obtained from a packet capture of their communication. [5 marks]

(2) Identify a method that lure a normal user of the server to your computer instead of the server machine. What information you can get from this? [5 marks]

(3) If the server is protected, what can youdo to penetrate the system from the client side? [8 marks]

D- Protecting your server: Now you have completed a first assessment of the network, what are your recommendations?

(1) Based on your results, you have identified that "Port knocking" method is important to implement on your server. Explain. [5 marks]

(2) Hackers will attempt to scan a machine looking for suitable vulnerabilities to exploit. In your own words explain what false positives and false negatives are in relation to a Network Intrusion Detection System (NIDS). [6 marks]

(3) Explain the difference between Intrusion Detection System IDS and Intrusion prevention System IPS. Suggest a recommendation for the scenario you have in hand. [5 marks]

(4) Evaluate the effectiveness of the following tools and specify which you will use. justify you answers. [5 marks]

- Firewall
- Snort
- iptable

(5) Based on your findings, document any other recommendation based on vulnerabilities and weaknesses. Your recommendations should be based on the scenario you are working on and the type of data and services involved. [10 marks]

Learning Outcomes

The following Learning outcomes will be addressed in this assignment:

- **LO1** Have a critical understanding of the principles of computer systems security;
- **LO2** evaluate security architecture and design and provide the means to enhance system security;
- **LO3** employ cryptography appropriately and critically reflect on its limitations;
- **LO5** Synthesise emerging trends through engagement and analysis with current research.

Instructions

- You should not exceed **2500 words** in total excluding references page and any appendix you can include.
- References should follow Harvard referencing.

Marking scheme:

Activity	What needs to be done	Max Mark
Information gathering	Ports and their weaknesses. justification with references to enforce your idea.	8 marks
	Which services are the most important to protect based on your scenario	6 marks
	For those services identify their weaknesses. (Justification and research)	6 marks
	Four services and their danger (Justification and research)	6 marks
Vulnerabilities	Data tampering - Exploit if possible (with explanation and research)	5 marks
	SQL Injection - Exploit if possible (with explanation and research)	5 marks
	XSS - Exploit if possible (with explanation and research)	5 marks
	Any other - Exploit if possible (with explanation and research)	5 marks
MiTM and Social	Sniffing network, what information it gives.	5 marks
	Luring a user to connect to pen tester machine	5 marks
	Any other methods?	8 marks
Server protection	Port knocking advantage (with justification and research)	5 marks
	NIDS and how it can be used (with justification and research)	6 marks
	IDS or IPS for your scenario (with justification and research)	5 marks
	Recommend a tool to use (Justify your answer)	5 marks
	Document any other recommendation that is critical to your scenario security based on your findings.	10 marks
	Technical contents total:	95 marks
Structure and ease of read	Your document should be easy to follow and understand by readers. You should have clear references to examples to justify your choices	5 marks
	Total	100 marks